

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: <b>Peng T. Ong</b>	§	Group Art Unit: <b>2136</b>
	§	
Serial No. <b>10/617,607</b>	§	Examiner: <b>Johnson, Carlton</b>
	§	
Filed: <b>July 11, 2003</b>	§	Customer No.: <b>50170</b>
	§	
For: <b>Method for Consolidation of</b>	§	
<b>User Directories</b>	§	

**Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450**

**ATTENTION: Board of Patent Appeals and Interferences**

**APPELLANT'S BRIEF (37 C.F.R. § 41.37)**

This Appeal Brief is in furtherance of the Notice of Appeal filed October 16, 2008 (37 C.F.R. § 41.31).

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Fee Transmittal.

## **I. Real Party in Interest**

The real party in interest in this appeal is the following party: International Business Machines Corporation.

## **II. Related Cases**

With respect to other appeals and interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

## **III. Jurisdiction**

The Board has jurisdiction under 35 U.S.C. § 134(a). The Examiner mailed a final rejection on September 16, 2008, setting a three-month shortened statutory period for response. The time for responding to the final rejection expired on December 16, 2008. Rule 134. A notice of appeal was filed on October 16, 2008. The time for filing an appeal brief is two months after the filing of a notice of appeal. Bd.R. 41.37(c). The time for filing an appeal brief expires on December 16, 2008. The appeal brief is being filed on December 4, 2008.

#### **IV. Table of Contents**

Real Party of Interest .....	2
Related Cases .....	2
Jurisdiction .....	2
Table of Contents .....	3
Table of Authorities .....	3
Status of Amendments .....	4
Grounds of Rejection to be Reviewed .....	4
Statement of Facts .....	4
Argument .....	8
Appendix .....	35
Claims .....	35
Claims Support and Drawing Analysis .....	42
Means or Step Plus Function Analysis .....	52
Evidence .....	54
Related Cases .....	54

#### **V. Table of Authorities**

NONE

## **VI. Status of Amendments**

No amendment was filed after final rejection.

## **VII. Grounds of Rejection to be Reviewed on Appeal**

The grounds of rejection to be reviewed on appeal are:

- The rejection of claims 1, 16, 17, and 21-27 under 35 U.S.C. § 112, first paragraph;
- The rejection of claims 1, 3-7, 9, 10, and 18-27 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schaeck et al. in view of Cotte, and further in view of Delany et al.; and
- The rejection of claims 16-17 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schaeck et al. in view of Cotte.

## **VIII. Statement of Facts**

1. In rejecting claims 1, 16, 17, and 21-27 under 35 U.S.C. § 112, first paragraph, the Final Office Action (pages 3-4) states that there is no support for the terms “coupling,” “separate,” or the phrase “coupling of a separate hardware security device.”

2. The present specification, at page 7, lines 2-3, recites that the access agent controller 235 ensures proper startup of the Access Agent 200 “upon an insertion of SOCI into the client machine.”
3. The present specification, at page 7, lines 17-18 (paragraph [0024]) states that the “SOCI is a hardware token capable of being connected to the user’s computer.”
4. The present specification, at page 13, line 1, states that the access agent controller identifies whether a SOCI is present in any of the Universal Serial Bus (USB) ports.
5. It is generally known that USB ports are used for coupling separate USB capable devices to a computing system.
6. In each of the 35 U.S.C. § 103(a) rejections of independent claims 1, 16, and 17, the Final Office Action alleges that there is no support for the features of a separate hardware device (see Final Office Action, pages 5, 11, 20, and 21).
7. In rejecting independent claims 1 and 18 under 35 U.S.C. § 103(a), the Final Office Action admits that Schaeck does not disclose a consolidated user directory (see Final Office Action, page 5), but alleges that Delany teaches this feature at paragraph [0113], lines 13-18 and paragraph [0129], lines 16-20.
8. In paragraph [0113] of Delany, the reference teaches:

With Group Manager 44, companies (or other entities) can allow individual users to do the following: (1) self-subscribe to and unsubscribe from groups, (2) view the groups that they are eligible to join or have joined, and (3) request subscription to groups that have access to the applications they need. Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly. Group Manager 44 also lets companies form dynamic groups specified by an LDAP filter. The ability to create and use dynamic groups is extremely valuable because it eliminates the administrative headache of continually keeping individual, static membership up-to-date. With dynamic group management features, users can be automatically added or removed if they meet the criteria specified by the LDAP filter. Dynamic groups also greatly enhance security since changes in user identities that disqualify someone from membership in a group are automatically reflected in the dynamic group membership.

9. In paragraph [0129] of Delany, the reference teaches:

When database manager 120 starts, it will read the directory server configuration file(s) and insert corresponding profile and agent objects to its internal tables for later reference. FIG. 3 shows database manager 120 in communication with profiles 122, 124, 126 and 128. Each profile corresponds to an agent. For example, profile 122 corresponds to agent 130, profile 124 corresponds to agent 132, profile 126 corresponds to agent 134, and profile 128 corresponds to

agent 136. Each agent is associated with a connection manager and a data store. For example, agent 130 is associated with connection manager 140 and data store 36a. Agent 132 is associated with connection manager 142 and data store 36b. Agent 134 is associated with connection manager 144 and data store 36c. Agent 136 is associated with connection manager 146 and data store 36d. In one embodiment, each of the data stores are LDAP directory servers with LDAP directories. In other embodiments, one or more of the data stores are LDAP directories and one or more of the data stores are other types of data stores (e.g. SQL servers) or others. In further embodiments, none of the data stores are LDAP directories.

10. In rejecting independent claims 1 and 18 under 35 U.S.C. § 103(a), the Final Office Action (page 6) further admits that the alleged combination of Schaeck and Delany does not disclose a complete listing of applications, but alleges that Cotte teaches this feature at paragraph [0116], lines 1-7.

11. In paragraph [0116] of Cotte, the reference teaches:

Furthermore it is possible to access a certain telecommunications portal in order to retrieve data about the different telecommunications web sites residing on that telecommunications portal in total, for instance about the structure of specific entities (natural persons or companies, etc.) corresponding to the telecommunications web sites on this telecommunications portal.

12. In rejecting independent claims 16 and 17, the Final Office Action again admits that Schaeck does not teach a complete listing of applications (see Final Office Action, pages 20 and 22), but alleges that the Cotte reference teaches this feature again citing paragraph [0016] (see Final Office Action, pages 21 and 22).

## **IX. Argument**

### **A. Rejection under 35 U.S.C. § 112, First Paragraph**

The Final Office Action, on pages 3-4, rejects claims 1, 16, 17, and 21-27 under 35 U.S.C. § 112, first paragraph as allegedly reciting subject matter which is not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. Specifically, the Final Office Action alleges that the specification does not provide support for the terms “coupling,” “separate,” or the phrase “coupling of a separate hardware security device” as they appear in these claims. This rejection is respectfully traversed.

Presented here for the first time, Appellant respectfully submits that the present specification provides sufficient support for these features at least in Figure 1 and on page 7, lines 2-3; page 7, lines 17-18; and page 13, line 1. Figure 1 clearly shows a separate Secure Object for Convenient Identification (SOCI)



device 120. Page 7, lines 2-3 recites that the access agent controller 235 ensures proper startup of the Access Agent 200 “upon an insertion of SOCI into the client machine.” Thus, the SOCI must be a separate device in order for it to be “inserted” into the client machine. Moreover, the insertion of the SOCI device is evidence of a “coupling” of the SOCI device with the client machine. Page 7, lines 17-18 (paragraph [0024]) further states, with reference to Figure 3, that the “SOCI is a hardware token capable of being connected to the user’s computer.” Moreover, on page 13, line 1, it is described that the access agent controller identifies whether a SOCI is present in any of the USB ports. As is generally known, USB ports are used for coupling separate USB capable devices to a computing system. In summary, these sections of the present specification clearly describe a separate hardware device, e.g., the SOCI hardware device, that is coupled to a data processing system, e.g., by insertion of the SOCI into the client machine, being “connected” to a user’s computer, or otherwise being “present” in a USB port of the data processing system.

Thus, even though the specification may not use the exact terms “coupling” or “separate,” it is clear to those “skilled in the relevant art” that the specification describes a separate SOCI device that is coupled to a client machine. Thus, the rejection of these claims is in error.

**B. Rejection under 35 U.S.C. § 103(a), Claims 1, 3-7, 9, 10, and 18-27**

The Final Office Action (page 4) rejects 1, 3-7, 9, 10, and 18-27 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Schaeck et al. (U.S. Patent Application Publication No. 2003/0163513) in view of Cotte (U.S. Patent Application Publication No. 2004/0013132), and further in view of Delany et al. (U.S. Patent Application Publication No. 2002/0013132). This rejection is respectfully traversed.

**1. Independent Claim 1**

Independent claim 1 reads as follows:

1. A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:

**receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user;**

identifying the plurality of applications accessible by the user by examining the authentication credential container associated with the user;

generating a view of the plurality of applications accessible by

the user, **wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications**; and

displaying the view to the administrator. (emphasis added)

As originally presented in the Response to Office Action filed April 30, 2008 and again on June 18, 2008 (pages 10-12), Appellant respectfully submits that neither Schaeck nor Cotte, either alone or in combination, teach or suggest at least the features emphasized above in claim 1. As presented for the first time herein, Appellant further submits that Delany et al. also does not teach or suggest at least these features, whether taken alone or in combination with Schaeck and Cotte.

Schaeck is directed to a mechanism for providing role based views of business web portals. With the mechanism of Schaeck, an aggregated service is comprised of one or more software resources. A role-specific portlet for each role supported by a particular one of the software resources is provided. A linkage between the role-specific portlets and the roles of the particular software resources is provided. At run time, a user role corresponding to a user of the aggregated services is obtained and a corresponding one of the role-specific portlets is programmatically selected to thereby provide a role-specific view of the aggregated service. The mechanism further determines which of the software resources to invoke to position the user's entry point into the aggregated service

and uses the obtained role to select a role specific view of the determined software resource.

While Schaeck teaches to aggregate portlets for a user into an aggregate portal page view (see Figure 7 of Schaeck), nowhere in Schaeck is there any teaching or suggestion regarding “receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user” as recited in claim 1. To the contrary, in Figure 7 of Schaeck it is clearly shown that the user is presented with available services, the user selects a service, and based on the user’s role, portlets associated with the service are selected and combined into an aggregate portal page that is presented to the user. Schaeck provides no teaching or suggestion regarding a separate hardware security device, let alone receiving credential information for each application of a plurality of applications that the user uses from the separate hardware security device in response to the separate hardware security device being coupled to a data processing system or receiving such credential information into an authentication credential container associated with the user.

Moreover, Schaeck does not teach that the view that is generated is a consolidated user directory that contains user authentication information across a

plurality of applications. To the contrary, the “view” that is generated in Schaeck is a portal page that has the portlets for a selected service. There is no teaching or suggestion in Schaeck that this portal page contains user authentication information across a plurality of applications. To the contrary, as described in paragraph [0073] of Schaeck, the portlets provide different interfaces for different user roles. In paragraph [0081] Schaeck teaches that the user’s role is determined based on the user’s login information, but this does not teach or suggest that the actual view that is generated in Schaeck contains user authentication information across a plurality of applications.

Cotte does not teach or suggest these features either, whether Cotte is taken alone or in combination with Schaeck. Cotte is cited as alleged teaching a plurality of applications at paragraph [0116]. Cotte is directed to a multiprotocol communications environment. In paragraph [0116] of Cotte, all that is taught is that it is possible to access a telecommunications portal in order to retrieve data about different telecommunications web sites residing on that telecommunications portal in total. There is nothing in Cotte that teaches or suggests the specific features of claim 1 discussed above with regard to Schaeck, i.e. a separate hardware device that is coupled to a data processing system; receiving, in response to a coupling of the separate hardware security device to the data processing system, credential information for each application of the plurality of applications

that the user uses from the separate hardware security device into an authentication credential container associated with the user; or a view that is generated is a consolidated user directory that contains user authentication information across a plurality of applications. Merely providing a telecommunications portal that provides information about telecommunications web sites has nothing to do with identifying a plurality of applications that a user may access from a separate hardware security device in response to such a device being coupled to a data processing system or that a view that is presented is a consolidated user directory that contains user authentication information across the plurality of applications.

The Final Office Action admits that Shaeck does not teach a consolidated user directory (Final Office Action, page 5) or a complete listing of applications (Final Office Action, page 6). The Final Office Action alleges that Cotte teaches a complete listing of applications in paragraph [0116] which has been addressed above and has been shown to not actually teach or suggest such a feature but instead simply a presentation of information about telecommunications web sites. The Final Office Action further alleges, at pages 5-6, that Delany discloses a consolidated user directory that contains user authentication information across a plurality of applications at paragraph [0113], lines 13-18 and paragraph [0129], lines 16-20 which read as follows:

[0113] With Group Manager 44, companies (or other entities) can allow individual users to do the following: (1) self-subscribe to and unsubscribe from groups, (2) view the groups that they are eligible to join or have joined, and (3) request subscription to groups that have access to the applications they need. Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly. Group Manager 44 also lets companies form dynamic groups specified by an LDAP filter. The ability to create and use dynamic groups is extremely valuable because it eliminates the administrative headache of continually keeping individual, static membership up-to-date. With dynamic group management features, users can be automatically added or removed if they meet the criteria specified by the LDAP filter. Dynamic groups also greatly enhance security since changes in user identities that disqualify someone from membership in a group are automatically reflected in the dynamic group membership.

[0129] When database manager 120 starts, it will read the directory server configuration file(s) and insert corresponding profile and agent objects to its internal tables for later reference. FIG. 3 shows database manager 120 in communication with profiles 122, 124, 126 and 128. Each profile corresponds to an agent. For example, profile 122 corresponds to agent 130, profile 124 corresponds to agent 132, profile 126 corresponds to agent 134, and profile 128 corresponds to agent 136. Each agent is associated with a connection manager and a data store. For example, agent 130 is associated with connection

manager 140 and data store 36a. Agent 132 is associated with connection manager 142 and data store 36b. Agent 134 is associated with connection manager 144 and data store 36c. Agent 136 is associated with connection manager 146 and data store 36d. In one embodiment, each of the data stores are LDAP directory servers with LDAP directories. In other embodiments, one or more of the data stores are LDAP directories and one or more of the data stores are other types of data stores (e.g. SQL servers) or others. In further embodiments, none of the data stores are LDAP directories.

As discussed in Responses filed April 30, 2008 and June 18, 2008 (page 13), these sections of Delany only teach that (1) with the Group Manager in Delany, a user may view the groups that they are eligible to join or have joined, view the groups that they are eligible to join or have joined, and request subscription to groups that have access to the applications they need; (2) groups may be created dynamically with an LDAP filter; (3) the database manager reads a configuration file and inserts profile and agent objects to its internal tables; (4) each profile corresponds to an agent and each agent is associated with a connection manager and a data store which may be an LDAP directory server. Nothing in these sections, or any other sections, of Delany teach or suggest generating a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of



applications. Moreover, nothing in Delany teaches or suggests the feature of receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user.

In Response to the above, the Examiner responds, on pages 2-3 of the Final Office Action, by alleging that there is no disclosure of a separate hardware device in the specification or original claims, and references the 35 U.S.C. § 112, first paragraph rejection discussed above. It has been shown above that the specification provides ample support for the recitation of a separate hardware device and the coupling of the separate hardware device to a data processing system. Thus, the Examiner's argument is in error. The Examiner then reiterates the allegations with regard to the Delany reference allegedly teaching a consolidated view (see Final Office Action, page 3). Again, it has been shown above that Delany in fact does not teach or suggest such features, especially in the portions of the Delany reference specifically cited by the Examiner as allegedly teaching these features.

Thus, for at least the reasons set forth above, Applicant respectfully submits that none of the cited references, Schaeck, Cotte, and Delany, whether taken alone or in combination, teaches or suggests the features of independent claim 1. Claims

3-7, 9, 10, and 21-27 depend from claim 1 and thus, are distinguished over the alleged combination of Schaeck, Cotte and Delany at least by virtue of their dependency. Accordingly, Appellant respectfully requests that the Board overturn the rejection of claims 1, 3-7, 9, 10, and 21-27 under 35 U.S.C. § 103(a).

In addition to the above, the alleged combination of references fails to teach or suggest the specific additional features presented in the dependent claims.

## **2. Dependent Claims 3 and 6**

With regard to claim 3, as presented here for the first time, Appellant respectfully submits that none of the cited references, whether taken alone or in combination, teaches or suggests removing access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user. Again, none of the cited references teach or suggest a view that is a consolidated user directory that contains user authentication information across the plurality of applications. Therefore, the references cannot possibly teach or suggest using such a view to remove access to an application.

The Final Office Action (page 7) alleges that these features are taught by Schaeck at paragraphs [0043] and [0068] with the exception of providing a complete listing of applications, which the Final Office Action again alleges is

taught by Cotte. Paragraphs [0043] and [0068] of Schaeck only teach that a service may have a number of different views established for the service and users with particular roles are provided with different views of the service. There is nothing in these sections of Schaeck that teach or suggest anything regarding using a view that is a consolidated user directory to remove access to an application, as recited in claim 3. Moreover, none of the other cited references teach or suggest such features.

Since the cited references do not teach or suggest the features of claim 3 as noted above, the cited references further cannot teach or suggest the features of claim 6, with regard to the removing being performed automatically, at least by virtue of the dependency of claim 6 from claim 3.

### **3. Dependent Claims 4, 5, and 7**

Regarding claim 4, as presented here for the first time, Appellant respectfully submits that none of the cited references, whether taken alone or in combination, teach or suggest creating a user account for a new application to be accessible by the user utilizing the generated view or injecting authentication information of the user account into the authentication credential container of the user. The Final Office Action (pages 8-10) again alleges that the view feature is taught by Schaeck at paragraphs [0043] and [0068], which have been addressed

above. The Final Office Action further references paragraph [0052] of Schaeck which only teaches that a composition tool may be used to combine fine grain services with a larger more general service. This does not provide any further teaching or suggestion relevant to the view feature of the claims.

With regard to the features of creating a user account for a new application using the view and injecting authentication information of the user account, the Final Office Action points to Delany, paragraphs [0108] and [0109] as allegedly teaching these features. While these paragraphs do mention the creation and deletion functions of user management, there is no teaching or suggestion in Delany regarding the specific feature of using a view that is a consolidated user directory that contains user authentication information across a plurality of applications to perform such creation or deletion or injecting authentication information into an authentication credential container of the user.

Since the cited references do not teach or suggest the features of claim 4 as noted above, the cited references further cannot teach or suggest the features of claims 5 and 7, with regard to the authentication credential container being stored at a server and the creation of the user account being performed either automatically or manually by an administrator, at least by virtue of the dependency of claims 5 and 7 from claim 4.

#### **4. Dependent Claim 9**

Regarding claim 9, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the authentication information is injected into the separate hardware security device. With regard to this feature, the Final Office Action (pages 10-11) again alleges that there is no support for the “separate hardware security device” in the present specification (see the 35 U.S.C. § 112, first paragraph rejection section above) and simply disregards this part of the claim. However, as shown above, there is ample support for this feature in the present specification and thus, the position taken by the Final Office Action is erroneous. There simply is no teaching in any of the references regarding injecting authentication information into a separate hardware security device.

#### **5. Dependent Claim 10**

Regarding claim 10, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest removing individual user directories for each application of the plurality of the applications accessible by the user. The Final Office Action (page 11) again points to paragraphs [0043] and [0068] of Schaeck and paragraphs [0108] and [0109] of Delany. The paragraphs of Schaeck cited by

the Final Office Action are just as irrelevant to these features as they are to the other features previously discussed. With regard to the cited portions of Delany, while Delany mentions a deletion function of user management, there is no teaching or suggestion in Delany regarding the specific features of removing individual user directories for each application of the plurality of the applications accessible by the user. Thus, any alleged combination of Delany with the other references still would not result in these features being taught or suggested.

#### **6. Dependent Claim 21**

With regard to claim 21, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teaches or suggests that the view comprises a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key. The Final Office Action (page 16) admits that Schaeck does not teach this feature, but alleges that Delany teaches these features in paragraphs [0361] and [0374]. First, as noted above, Delany does not teach the view recited in independent claim 1 as discussed above, this view being the view referenced in claim 21. Second, the cited sections of Delany teaches that a certificate may include fields specifying a key algorithm, a public

key value, and a certificate serial number (see Delany, paragraph [0361]) .

However, nowhere in Delany is there any teaching of a view that has a list of keys with each entry in the list corresponding to a different key employed by a user.

Thus, even though Delany teaches a public key value, a key algorithm, and a certificate serial number, Delany fails to teach or suggest these other features of claim 21 which are also not taught or suggested by the other cited references.

## **7. Dependent Claim 22**

With regard to claim 22, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the view comprises a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user. The Final Office Action (page 17), alleges that these features are taught by Schaeck at paragraphs [0108] and [0109] because Schaeck teaches a user profile. While Schaeck may teach a user profile, this does not teach that the view, which is a consolidated user directory as recited in claim 1, comprises such a profile. Thus, the alleged combination of references still fails to teach or suggest the specific features of claim 22.

## **8. Dependent Claim 23**

Regarding claim 23, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the view comprises a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application. The Final Office Action (page 17) alleges that these features are taught by Schaeck in paragraphs [0043] and [0068]. Paragraph [0043] merely provides examples of a role specific view of a service. Paragraph [0068] merely describes the defining of separate role views for services. Neither of these portions of Schaeck, or any other portion of Schaeck, teaches or suggests the specific features of a list of certificate-enabled applications accessible by a user with entries in the list corresponding to different certificate enabled applications and each entry identifying a user name and a last login attempt of the user. These features are not even really addressed by the Final Office Action but instead are merely disregarded by pointing to the same general sections of Schaeck previously cited without any analysis as to how they apply to the specific features of the claim. There simply is no teaching in Schaeck, or any of the other cited references, regarding the specific features of claim 23.



## **9. Dependent Claim 24**

Regarding claim 24, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the view comprises a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application. Similar to the rejection of claim 23 above, the Final Office Action (page 17) cites the same sections of Schaeck as allegedly teaching these features but then further states that Delany teaches the last login attempt of the user feature at paragraphs [0428] and [0429]. These paragraphs of Delany generally teach the “logging” of successful and unsuccessful login attempts. However, there is no teaching or suggestion in Delany regarding a view, such as that recited in claim 1 and claim 24 by its dependency, having the entries for each enterprise application and these entries having the user name and last login attempt, as recited in claim 24. The specific arrangement of elements set forth in claim 24 is neither taught nor suggested by the alleged combination of references.

#### **10. Dependent Claim 25**

Regarding claim 25, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the view comprises a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application. The Final Office Action (page 18) alleges that these features are taught by Schaeck in paragraphs [0043] and [0068] which have been addressed above. As noted above, these sections only discuss examples of different role views of a service and provide no teaching or suggestion regarding any list of personal applications, let alone such a list that has entries that correspond to different personal applications with each entry identifying a number of accounts connected to the personal application. There simply is no correlation between the paragraphs of Schaeck and the features of claim 25.

#### **11. Dependent Claim 26**

Regarding claim 26, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the view comprises user selectable graphical

user interface elements for invoking a function to update the profile and for invoking a function to reset the profile. The Final Office Action (page 19) points to paragraphs [0043], [0044], and [0066] of Schaeck as allegedly teaching these features. Paragraph [0043] provides examples of role based views of a service, paragraph [0044] teaches “user-facing” web applications having user interfaces for communicating with a user, and paragraph [0066] teaches the modification of user profiles. However, nowhere in Schaeck is there any teaching or suggestion regarding a view, such as that recited in claims 1 and 26, having selectable graphical user interface elements to update the profile portion of the view and for invoking a reset of the profile.

## **12. Dependent Claim 27**

Regarding claim 27, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest that the view comprises a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications. Again, the Final Office Action (page 19) points to paragraphs [0043], [0044], and [0066] as allegedly teaching these features. As noted above with regard to the rejection of claim 26, Schaeck in fact does not teach the specific features of claim 27 in a similar way that Schaeck

does not teach the features of claim 26. While Schaeck may generally teach the modification of user profiles, Schaeck provides no teaching or suggestion regarding the specific arrangement of features set forth in claim 27.

### **13. Independent Claim 18**

With regard to independent claim 18, this claim recites:

18. A method for providing a system administrator with a consolidated directory of a plurality of applications accessible by a user, the method comprising:

- identifying the plurality of applications accessible by the user by examining authentication credential container of the user;
- generating a directory of the plurality of applications accessible by the user; and
- displaying the directory to the administrator;

the directory comprising:

- a name of the user;**
- a list of keys employed by the user also detailing the type and serial number of each key;**
- a profile of the user detailing a role of the user, a name of the user, an email address of the user, a department of the user, an employee ID of the user, and any additional attributes of the user that have been specified;**
- a means of updating and resetting the profile;**

**a list of certificate-enabled applications accessible by the user also specifying a user name of the user and a last login attempt of the user;**

**a means of deleting the user name of the user;**

**a list of enterprise applications accessible by the user also specifying a user name of the user and a last login attempt of the user; and**

**a list of personal applications accessible by the user also specifying a number of accounts connected to each personal application. (emphasis added)**

As presented here for the first time, Appellant respectfully submits that claim 18 recites features similar to that of dependent claims 21-27 but in combination with each other. For similar reasons as set forth above with regard to claims 21-27, none of the cited references, whether taken alone or in combination, teach or suggest the features of claim 18 emphasized above. That is, none of the cited references teach or suggest these features separately as discussed above with regard to each individual dependent claim 21-27. Furthermore, none of the cited references teach or suggest the combination of these features as it is set forth in claim 18. Therefore, any alleged combination of the references still would not result in these features being taught or suggested, especially when these features are combined in the manner set forth in claim 18.

#### **14. Dependent Claim 19**

Regarding Claim 19, as presented here for the first time, Appellant respectfully submits that none of the cited references, either alone or in combination, teach or suggest a specification of a password for each certificate-enabled application, each enterprise application, and each personal application. The Final Office Action (page 15) alleges that these features are taught by Schaeck in paragraph [0059]. Paragraph [0059] teaches the encrypting of passwords for sub-services of an aggregate service. While Schaeck is teaches passwords for sub-services of an aggregate service, Schaeck does not teach or suggest a directory that has a password for each certificate-enabled application, each enterprise application, and each personal application in the directory. None of the other cited references teach or suggest these features either and thus, any alleged combination of these references still would not result in these features being taught or suggested.

#### **C. Rejection under 35 U.S.C. § 103(a), Claims 16, 17**

The Final Office Action (pages 19-22) rejects claims 16-17 under 35 U.S.C. §103(a) as being allegedly unpatentable over Schaeck et al. (U.S. Patent Application Publication No. 2003/0163513) in view of Cotte (U.S. Patent

Application Publication No. 2004/0013132). This rejection is respectfully traversed.

### **1. Independent Claim 16**

As discussed in the Responses filed April 30, 2008 and June 18, 2008 (pages 10-12), independent Claim 16 recites receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user. As discussed at length above with regard to claim 1, neither Schaeck nor Cotte, either alone or in combination, teach or suggest such features.

As discussed above, in Figure 7 of Schaeck it is clearly shown that the user is presented with available services, the user selects a service, and based on the user's role, portlets associated with the service are selected and combined into an aggregate portal page that is presented to the user. Schaeck provides no teaching or suggestion regarding a separate hardware security device, let alone receiving credential information for each application of a plurality of applications that the user uses from the separate hardware security device in response to the separate hardware security device being coupled to a data processing system or receiving

such credential information into an authentication credential container associated with the user.

Cotte likewise does not teach or suggest these features either, whether Cotte is taken alone or in combination with Schaeck. As discussed above, Cotte teaches that it is possible to access a telecommunications portal in order to retrieve data about different telecommunications web sites residing on that telecommunications portal in total. However, there is nothing in Cotte that teaches or suggests the specific features of claim 16 discussed above with regard to Schaeck, i.e. a separate hardware device that is coupled to a data processing system; receiving, in response to a coupling of the separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user. Merely providing a telecommunications portal that provides information about telecommunications web sites has nothing to do with identifying a plurality of applications that a user may access from a separate hardware security device in response to such a device being coupled to a data processing system or that a view that is presented is a consolidated user directory that contains user authentication information across the plurality of applications.



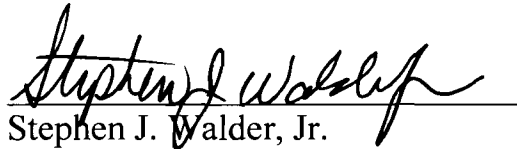
In view of the above, Appellant respectfully submits that neither Schaeck nor Cotte, either alone or in combination, teaches or suggests the features of claim 16. Accordingly, Appellants respectfully request that the Board overturn the rejection of claim 16 under 35 U.S.C. § 103(a).

## **2. Independent Claim 17**

As discussed in the Responses filed April 30, 2008 and June 18, 2008 (pages 10-12), similar to claim 16 above, claim 17 also recites receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of a plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user. Thus, claim 17 is likewise defining over the alleged combination of Schaeck and Cotte for similar reasons as set forth above with regard to claims 1 and 16 above. Accordingly, Appellant respectfully requests that the Board overturn the rejection of claim 17 under 35 U.S.C. § 103(a).

In view of the above, Appellants respectfully submit that the features of claims 1, 3-7, 9, 10, and 16-27 of the present application are not taught or suggested by the cited references. Accordingly, Appellants request that the Board of Patent Appeals and Interferences overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

A handwritten signature in black ink, reading "Stephen J. Walder, Jr.", is written over a horizontal line.

Stephen J. Walder, Jr.

Reg. No. 41,534

**Walder Intellectual Property Law, P.C.**

17330 Preston Road, Suite 100B

Dallas, TX 75252

Phone: (972) 380-9475

Fax: (972) 733-1575

Email: [swalder@walderiplaw.com](mailto:swalder@walderiplaw.com)

ATTORNEY FOR APPELLANT

## **X. Appendix**

### **A. Claims**

1. (Rejected) A method, in a data processing system, for providing a system administrator with a view of a plurality of applications accessible by a user, comprising:

receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user;

identifying the plurality of applications accessible by the user by examining the authentication credential container associated with the user;

generating a view of the plurality of applications accessible by the user, wherein the view is a consolidated user directory that contains user authentication information across the plurality of applications; and

displaying the view to the administrator.

2. (Canceled)

3. (Rejected) The method of claim 1 further comprising removing access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user.
4. (Rejected) The method of claim 1 further comprising:  
creating a user account for a new application to be accessible by the user  
utilizing the generated view; and  
injecting authentication information of the user account into the authentication credential container of the user.
5. (Rejected) The method of claim 4 wherein the authentication credential container is stored at a server.
6. (Rejected) The method of claim 3 wherein the removing is performed automatically.
7. (Rejected) The method of claim 4 wherein the creating the user account is performed either automatically or manually by an administrator.
8. (Canceled)

9. (Rejected) The method of claim 4 wherein the authentication information is injected into the separate hardware security device.

10. (Rejected) The method of claim 1 further comprising removing individual user directories for each application of the plurality of the applications accessible by the user.

11-15. (Canceled)

16. (Rejected) A method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user, comprising:

receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of the plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user;

identifying the plurality of applications accessible by the user by examining an authentication credential container associated with the user;

generating a list of the plurality of applications accessible by the user; and displaying the list to the administrator.

17. (Rejected) A method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user together with any user names and passwords used in connection with those applications, comprising:

receiving, in response to a coupling of a separate hardware security device to the data processing system, credential information for each application of a plurality of applications that the user uses from the separate hardware security device into an authentication credential container associated with the user;

identifying the plurality of applications accessible by the user and any user names and passwords used in connection with the plurality of applications by examining an authentication credential container associated with the user;

generating a list of the plurality of applications accessible by the user together with any user names and passwords used in connection with the plurality of applications; and

displaying the list to the administrator.

18. (Rejected) A method for providing a system administrator with a consolidated directory of a plurality of applications accessible by a user, the method comprising:

identifying the plurality of applications accessible by the user by examining

authentication credential container of the user;

generating a directory of the plurality of applications accessible by the user;

and

displaying the directory to the administrator;

the directory comprising:

a name of the user;

a list of keys employed by the user also detailing the type and serial number of each key;

a profile of the user detailing a role of the user, a name of the user, an email address of the user, a department of the user, an employee ID of the user, and any additional attributes of the user that have been specified;

a means of updating and resetting the profile;

a list of certificate-enabled applications accessible by the user also specifying a user name of the user and a last login attempt of the user;

a means of deleting the user name of the user;

a list of enterprise applications accessible by the user also specifying a user name of the user and a last login attempt of the user; and

a list of personal applications accessible by the user also specifying a number of accounts connected to each personal application.

19. (Rejected) The method of claim 18, further comprising:

a specification of a password for each certificate-enabled application, each enterprise application, and each personal application.

20. (Rejected) The method of claim 18, further comprising:

means for a system administrator to add one or more applications to the lists of the certificate-enabled applications, the enterprise applications, or the personal applications of the user; and

means for a system administrator to delete one or more applications from the lists of the certificate-enabled applications, the enterprise applications, or the personal applications.

21. (Rejected) The method of claim 1, wherein the view comprises:

a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key.

22. (Rejected) The method of claim 1, wherein the view comprises:

a profile of the user detailing a role of the user, a name of the user, contact



information for the user, and employment information for the user.

23. (Rejected) The method of claim 1, wherein the view comprises:

a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application.

24. (Rejected) The method of claim 1, wherein the view comprises:

a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application.

25. (Rejected) The method of claim 1, wherein the view comprises:

a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application.

26. (Rejected) The method of claim 22, wherein the view comprises:  
user selectable graphical user interface elements for invoking a function to  
update the profile and for invoking a function to reset the profile.

27. (Rejected) The method of claim 23, wherein the view comprises:  
a user selectable graphical user interface element for invoking a function to  
delete a user name of the user from the list of certificate-enabled applications.

#### **B. Claims Support and Drawing Analysis**

1. A method, in a data processing system, for providing a system administrator  
with a view of a plurality of applications accessible by a user {e.g., **paragraph**  
**[0046], lines 3-6**}, comprising:

receiving, in response to a coupling {e.g., **paragraph [0023], lines 2-3;**  
**paragraph [0024], lines 2-3; paragraph [0033], lines 10-15; paragraph [0035],**  
**lines 1-3; paragraph [0038], lines 1-3; paragraph [0045], lines 5-6**} of a  
separate hardware security device {e.g., **SOCI device 120 in Figure 1;**  
**paragraph [0023], lines 2-3; paragraph [0024], lines 2-3**} to the data processing  
system {e.g., **paragraph [0023], line 7; paragraph [0024], lines 11-14;**  
**paragraph [0025], lines 1-3; processing system in Figure 6**}, credential  
information {e.g., **paragraph [0024], lines 18-20; paragraph [0035], lines 12-**

**14; paragraph [0043], lines 2-3}** for each application of the plurality of applications that the user uses **{e.g., paragraph [0033], lines 1-3}** from the separate hardware security device **{e.g., paragraph [0033], lines 22-26; paragraph [0038], lines 3-4; paragraph [0040], lines 1-2; paragraph [0046], lines 1-3}** into an authentication credential container **{e.g., paragraph [0042], lines 7-8; paragraph [0048], lines 1-3}** associated with the user;

identifying the plurality of applications accessible by the user **{e.g., paragraph [0046], lines 3-6; original claim 1}** by examining the authentication credential container associated with the user **{e.g., paragraph [0048], lines 5-6; original claim 1}**;

generating a view **{e.g., see Figure 7}** of the plurality of applications accessible by the user, wherein the view is a consolidated user directory **{e.g., see Figure 7; original claim 2}** that contains user authentication information across the plurality of applications **{e.g., paragraph [0046], lines 6-8}**; and

displaying the view to the administrator **{e.g., paragraph [0046], lines 8-9}**.

3. The method of claim 1 further comprising removing access to an application from the plurality of the applications by utilizing the view of the plurality of the applications accessible by the user **{e.g., paragraph [0047], lines 1-7; original claim 3}**.

4. The method of claim 1 further comprising:  
  
creating a user account for a new application to be accessible by the user  
  
utilizing the generated view **{e.g., paragraph [0048], lines 1-6; original claim 4}**;  
  
and  
  
injecting authentication information of the user account into the  
  
authentication credential container of the user **{e.g., paragraph [0048], lines 1-6;  
original claim 4}**.
5. The method of claim 4 wherein the authentication credential container is  
  
stored at a server **{e.g., paragraph [0048], line 3; original claim 5}**.
6. The method of claim 3 wherein the removing is performed automatically  
  
**{e.g., paragraph [0049], lines 1-2; original claim 6}**.
7. The method of claim 4 wherein the creating the user account is performed  
  
either automatically **{e.g., paragraph [0045], lines 1-5; original claim 7}** or  
  
manually by an administrator **{e.g., paragraph [0045], lines 1-5; paragraph  
[0049], lines 1-2; original claim 8}**.
9. The method of claim 4 wherein the authentication information is injected

into the separate hardware security device {e.g., paragraph [0035], lines 15-17; paragraph [0036], lines 3-8 and 13-15; paragraph [0042]; paragraph [0045], lines 5-6; paragraph [0048], lines 3-6; original claim 9}.

10. The method of claim 1 further comprising removing individual user directories for each application of the plurality of the applications accessible by the user {e.g., paragraph [0046], lines 12-14; original claim 10}.

16. A method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user {e.g., paragraph [0046], lines 3-6}, comprising:

receiving, in response to a coupling {e.g., paragraph [0023], lines 2-3; paragraph [0024], lines 2-3; paragraph [0033], lines 10-15; paragraph [0035], lines 1-3; paragraph [0038], lines 1-3; paragraph [0045], lines 5-6} of a separate hardware security device {e.g., SOCI device 120 in Figure 1; paragraph [0023], lines 2-3; paragraph [0024], lines 2-3} to the data processing system {e.g., paragraph [0023], line 7; paragraph [0024], lines 11-14; paragraph [0025], lines 1-3; processing system in Figure 6}, credential information {e.g., paragraph [0024], lines 18-20; paragraph [0035], lines 12-14; paragraph [0043], lines 2-3} for each application of the plurality of applications that the user

uses {e.g., **paragraph [0033], lines 1-3**} from the separate hardware security device {e.g., **paragraph [0033], lines 22-26; paragraph [0038], lines 3-4; paragraph [0040], lines 1-2; paragraph [0046], lines 1-3**} into an authentication credential container associated with the user {e.g., **paragraph [0042], lines 7-8; paragraph [0048], lines 1-3**};

identifying the plurality of applications accessible by the user {e.g., **paragraph [0046], lines 3-6; original claim 1**} by examining an authentication credential container associated with the user {e.g., **paragraph [0048], lines 5-6; original claim 1**};

generating a list of the plurality of applications accessible by the user {e.g., see “**Certificate-Enabled Applications**,” “**Enterprise Applications**,” and “**Personal Applications**” in **Figure 7**}; and displaying the list to the administrator {e.g., **paragraph [0046], lines 8-9**}.

17. A method, in a data processing system, for providing a system administrator with a list of a plurality of applications accessible by a user together with any user names and passwords used in connection with those applications {e.g., **paragraph [0046], lines 3-6**}, comprising:

receiving, in response to a coupling {e.g., **paragraph [0023], lines 2-3; paragraph [0024], lines 2-3; paragraph [0033], lines 10-15; paragraph [0035],**

**lines 1-3; paragraph [0038], lines 1-3; paragraph [0045], lines 5-6}** of a separate hardware security device **{e.g., SOCI device 120 in Figure 1; paragraph [0023], lines 2-3; paragraph [0024], lines 2-3}** to the data processing system **{e.g., paragraph [0023], line 7; paragraph [0024], lines 11-14; paragraph [0025], lines 1-3; processing system in Figure 6}**, credential information **{e.g., paragraph [0024], lines 18-20; paragraph [0035], lines 12-14; paragraph [0043], lines 2-3}** for each application of a plurality of applications that the user uses **{e.g., paragraph [0033], lines 1-3}** from the separate hardware security device **{e.g., paragraph [0033], lines 22-26; paragraph [0038], lines 3-4; paragraph [0040], lines 1-2; paragraph [0046], lines 1-3}** into an authentication credential container associated with the user **{e.g., paragraph [0042], lines 7-8; paragraph [0048], lines 1-3}**;

identifying the plurality of applications accessible by the user **{e.g., paragraph [0046], lines 3-6; original claim 1}** and any user names and passwords used in connection with the plurality of applications by examining an authentication credential container associated with the user **{e.g., paragraph [0048], lines 5-6; original claim 1}**;

generating a list of the plurality of applications accessible by the user together with any user names and passwords used in connection with the plurality of applications **{e.g., see “Certificate-Enabled Applications,” “Enterprise**

**Applications,” and “Personal Applications” in Figure 7}; and**

displaying the list to the administrator {e.g., paragraph [0046], lines 8-9}.

18. A method for providing a system administrator with a consolidated directory of a plurality of applications accessible by a user {e.g., paragraph [0046], lines 3-6}, the method comprising:

identifying the plurality of applications accessible by the user {e.g., paragraph [0046], lines 3-6; original claim 1} by examining authentication credential container of the user {e.g., paragraph [0048], lines 5-6; original claim 1};

generating a directory of the plurality of applications accessible by the user {e.g., see Figure 7} and that contains user authentication information across the plurality of applications {e.g., paragraph [0046], lines 6-8}

displaying the directory to the administrator {e.g., paragraph [0046], lines 8-9};

the directory {e.g., see Figure 7} comprising:

a name of the user {e.g., see “Peirce, Jennifer I.” in Figure 7};

a list of keys employed by the user also detailing the type and serial number of each key {e.g., see “Keys” in Figure 7};

a profile of the user detailing a role of the user, a name of the user, an email



address of the user, a department of the user, an employee ID of the user, and any additional attributes of the user that have been specified {e.g., see **“Profile” in Figure 7**};

a means of updating and resetting the profile {e.g., see **“Update Profile” button and “Reset Form” button in Figure 7**};

a list of certificate-enabled applications accessible by the user also specifying a user name of the user and a last login attempt of the user {e.g., see **“Certificate-Enabled Applications” in Figure 7**};

a means of deleting the user name of the user {e.g., see **“Delete User Name” button in Figure 7**};

a list of enterprise applications accessible by the user also specifying a user name of the user and a last login attempt of the user {e.g., see **“Enterprise Applications” in Figure 7**}; and

a list of personal applications accessible by the user also specifying a number of accounts connected to each personal application {e.g., see **“Personal Applications” in Figure 7**}.

19. The method of claim 18, further comprising:

a specification of a password for each certificate-enabled application, each enterprise application, and each personal application {e.g., **paragraph [0023], line**

**24-26; paragraph [0025], lines 12-14; paragraph [0026], lines 14-15; paragraph [0033], lines 17-33}.**

21. The method of claim 1, wherein the view comprises:

a list of keys employed by the user, wherein each entry in the list corresponds to a different key employed by the user, and wherein each entry identifies a type of the corresponding key and a serial number of the corresponding key {e.g., see **“Keys” in Figure 7**}.

22. The method of claim 1, wherein the view comprises:

a profile of the user detailing a role of the user, a name of the user, contact information for the user, and employment information for the user {e.g., see **“Profile” in Figure 7**}.

23. The method of claim 1, wherein the view comprises:

a list of certificate-enabled applications accessible by the user, wherein each entry in the list corresponds to a different certificate-enabled application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding certificate-enabled application {e.g., see **“Certificate-Enabled Applications” in Figure 7**}.

24. The method of claim 1, wherein the view comprises:

a list of enterprise applications accessible by the user, wherein each entry in the list corresponds to a different enterprise application, and wherein each entry identifies a user name of the user and a last login attempt of the user for the corresponding enterprise application {e.g., see **“Enterprise Applications” in Figure 7**}.

25. The method of claim 1, wherein the view comprises:

a list of personal applications accessible by the user, wherein each entry in the list corresponds to a different personal application, and wherein each entry identifies a number of accounts connected to the corresponding personal application {e.g., see **“Personal Applications” in Figure 7**}.

26. The method of claim 22, wherein the view comprises:

user selectable graphical user interface elements for invoking a function to update the profile and for invoking a function to reset the profile {e.g., see **“Update Profile” button and “Reset Form” button in Figure 7**}.

27. The method of claim 23, wherein the view comprises:

a user selectable graphical user interface element for invoking a function to delete a user name of the user from the list of certificate-enabled applications {e.g., see **“Delete User Name” button in Figure 7**}.

**C. Means or Step Plus Function Analysis**

18. A method for providing a system administrator with a consolidated directory of a plurality of applications accessible by a user {e.g., **paragraph [0046], lines 3-6**}, the method comprising:

identifying the plurality of applications accessible by the user {e.g., **paragraph [0046], lines 3-6; original claim 1**} by examining authentication credential container of the user {e.g., **paragraph [0048], lines 5-6; original claim 1**};

generating a directory of the plurality of applications accessible by the user {e.g., see **Figure 7**} and that contains user authentication information across the plurality of applications {e.g., **paragraph [0046], lines 6-8**}

displaying the directory to the administrator {e.g., **paragraph [0046], lines 8-9**};

the directory {e.g., see **Figure 7**} comprising:

a name of the user {e.g., see **“Peirce, Jennifer I.” in Figure 7**};

a list of keys employed by the user also detailing the type and serial number of each key {e.g., see **“Keys” in Figure 7**};

a profile of the user detailing a role of the user, a name of the user, an email address of the user, a department of the user, an employee ID of the user, and any additional attributes of the user that have been specified {e.g., see **“Profile” in Figure 7**};

a means of updating and resetting the profile {e.g., see **“Update Profile” button and “Reset Form” button in Figure 7**};

a list of certificate-enabled applications accessible by the user also specifying a user name of the user and a last login attempt of the user {e.g., see **“Certificate-Enabled Applications” in Figure 7**};

a means of deleting the user name of the user {e.g., see **“Delete User Name” button in Figure 7**};

a list of enterprise applications accessible by the user also specifying a user name of the user and a last login attempt of the user {e.g., see **“Enterprise Applications” in Figure 7**}; and

a list of personal applications accessible by the user also specifying a number of accounts connected to each personal application {e.g., see **“Personal Applications” in Figure 7**}.

**D. Evidence**

NONE

**E. Related Cases**

NONE